IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

ARIEL OLIVER, individually and on behalf of all others similarly situated, Plaintiff, v. NOOM, INC., Defendant.	Case No. 2:22-cv-1857-WSS **JURY TRIAL DEMANDED**

FIRST AMENDED COMPLAINT - CLASS ACTION

Plaintiff Ariel Oliver ("Plaintiff"), individually and on behalf of all others similarly situated, hereby files this first amended class action complaint against Defendant Noom, Inc. ("Defendant" or "Noom"), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against Noom for wiretapping the electronic communications of visitors to its website, www.noom.com. Noom procures third-party vendors, such as FullStory, to embed snippets of JavaScript computer code ("Session Replay Code") on Noom's website, which then deploys on each website visitor's internet browser for the purpose intercepting and recording the website visitor's electronic communications with Noom's website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time ("Website Communications"). These third-party vendors (collectively, "Session Replay Providers") create and deploy the Session Replay Code at Noom's request.

2. After intercepting and capturing the Website Communications, Noom and the Session Replay Providers use those Website Communications to recreate website visitors' entire visit to www.noom.com. The Session Replay Providers create a video replay of the user's behavior on the website and provide it to Noom for analysis. Noom's procurement of the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of "looking over the shoulder" of each visitor to Noom's website for the entire duration of their website interaction.

3. Noom's conduct violates the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5701, *et. seq*., and constitutes an invasion of the privacy rights of website visitors.

4. Plaintiff brings this action individually and on behalf of a class of all Pennsylvania citizens whose Website Communications were intercepted through Noom's procurement and use of Session Replay Code embedded on www.noom.com, as well as its subpages, and seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys' fees and costs.

PARTIES

5. Plaintiff Ariel Oliver is a citizen of the Commonwealth of Pennsylvania, and at all times relevant to this action, resided and was a citizen of Pennsylvania. Plaintiff currently resides and is domiciled in Washington County, Pennsylvania. Plaintiff is a citizen of Pennsylvania.

6. Defendant Noom, Inc. is a corporation organized under the laws of Delaware, and its principal place of business in New York, New York. Defendant is a citizen of New York.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including Plaintiff, is a citizen of a state different than Defendant.

8. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiff's claims and harm occurred in Pennsylvania. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Pennsylvania while they were located within Pennsylvania. At all relevant times, Defendant targeted its goods and services to Pennsylvania citizens, and knew that its practices would directly result in collection of information from Pennsylvania citizens while those citizens browse www.noom.com from devices located in Pennsylvania. Defendant chose to avail itself of the business opportunities of marketing and selling its services in Pennsylvania and collecting real-time data from website visit sessions initiated by Pennsylvanians while located in Pennsylvania, and the claims and harm alleged herein specifically arise from those activities.

9. Noom also knows that many users visit and interact with Noom's website while they are physically present in Pennsylvania. Noom's website servers are capable of collecting user location data from a user's device such that Noom is continuously made aware that its website is being visited by people located in Pennsylvania, and that such website visitors are being wiretapped in violation Pennsylvania statutory and common law.

10. Finally, Noom spends millions of dollars on advertising across the country (including Pennsylvania).[1] Noom's successful advertising campaign has resulted in a robust market for its services throughout the United States (including Pennsylvania). Noom has over 45 million users and generates hundreds of millions of dollars in revenue.[2]

11. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District. Further, Pennsylvania has the greatest material interest in protecting the citizens in the Commonwealth of Pennsylvania, and enforcing the Pennsylvania Wiretapping and Electronic Surveillance Control Act given that the interception of Plaintiff's and Class Member's communications occurred from within the borders of the Commonwealth.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

12. The "world's most valuable resource is no longer oil, but data."[3]

13. In 2022, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data (*i.e.*, customers' purchase histories and product usage information), and attitudinal data (*i.e.*, data on

[1] Pathmatics, *Noom Spent More Than $21M on Digital Ads in the U.S. in January 2022*, Derived from Data News (Mar. 2, 2022), https://dfdnews.com/2022/03/02/noom-spent-more-than-21m-on-digital-ads-in-the-u.s.-in-january-2022/#:~:text=Between%20January%201%2C%202022%20through,about%20%248.9M%20on%20ads.

[2] Maya Robertson, *Noom Revenue and Usage Statistics*, Mobile Marketing Trends (Aug. 1, 2022), https://mobilemarketingreads.com/noom-revenue-and-usage-statistics-2021/.

[3] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

consumer satisfaction) from consumers.[4] This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.[5]

14. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[6]

15. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[7] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[8]

16. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[9]

---

[4] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, Business News Daily (Aug. 5, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.
[5] *Id.*
[6] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.
[7] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecd-ilibrary.org/docserver/5k486qtxldmq-en.pdf.
[8] *Id.* at 25.
[9] *Id.*

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

17. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that "a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[10]

18. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.[11] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[12]

19. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

20. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[13]

---

[10] Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/.

[11] *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html.

[12] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

[13] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/.

21. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[14]

22. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[15]

C. How Session Replay Code Works.

23. Session Replay Code, such as that implemented on www.noom.com, enables website operators to record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by recording website visitors "as they click, scroll, type or navigate across different web pages."[16]

24. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website

[14] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confused-and-feeling-lack-of-control-over-their-personal-information/.

[15] Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[16] Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/.

operator, or has not finished submitting the data to the website operator.[17] As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."[18]

25. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of actions the user takes. When a website delivers Session Replay Code to a user's browser, the browser will follow the code's instructions by sending responses in the form of "event" data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

26. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through the website. In order to permit a reconstruction of a user's visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

27. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

---

[17] *Id.*

[18] Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0.

28. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions."[19]

29. Because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.[20]

30. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a "submit" or "enter" button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

31. Session Replay Code does not necessarily anonymize user sessions, either.

---

[19] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

[20] *Id.*

32. First, if a user's entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

33. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

34. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.[21]

35. Session Replay Providers often create "fingerprints" that are unique to a particular user's combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

36. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user's other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

37. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.[22] Indeed, "[t]he more copies of

[21] *Id.*; *see also FS.identify – Identifying users*, FullStory, https://help.fullstory.com/hc/en-us/articles/360020828113, (last visited Mar. 29, 2023).
[22] Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720.

sensitive information that exist, the broader the attack surface, and when data is being collected [ ] it may not be stored properly or have standard protections" increasing "the overall risk that data will someday publicly leak or be breached."[23]

38. The privacy concerns arising from Session Replay Code is not theoretical or imagined. The CEO and founder of LOKKER, a provider of data privacy and compliance solutions has said "[consumers] should be concerned" about the use of Session Replay Code because "they won't know these tools are operating 'behind the scenes' of their site visit" and "even if the company disclosed that they are using these tools, consumers wouldn't likely be able to opt-out and still use the site."[24]

39. Indeed, the news is replete with examples of the dangers of Session Replay Code. For example, in 2019, the App Analyst, a mobile expert who writes about his analyses of popular apps, found that Air Canada's iPhone app wasn't properly masking the session replays they were sent, exposing unencrypted credit card data and password information.[25] This discovery was made just weeks after Air Canada said its app had a data breach, exposing 20,000 profiles.[26]

40. Further, multiple companies have removed Session Replay Code from their websites after it was discovered the Session Replay Code captured highly sensitive information. For instance, in 2017, Walgreens stopped sharing data with a Session Replay Provider after it was

---

[23] Lily Hay Newman, *Covert 'Replay Sessions' Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/.

[24] Mark Huffner, *Is 'session replay software' a privacy threat or just improving your web experience*, CONSUMER AFFAIRS (Oct. 25, 2022), https://www.consumeraffairs.com/news/is-session-replay-software-a-privacy-threat-or-just-improving-your-web-experience-102522.html.

[25] Zach Whittaker, Many Popular iPhone Apps Secretly Record Your Screen Without Asking, TECHCRUNCH (Feb. 6, 2019), https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/.

[26] *Id.*

discovered that the Session Replay provider gained access to website visitors' sensitive information.[27] Indeed, despite Walgreens' extensive use of manual redactions for displayed and inputted data, the Session Replay Provider still gained access to full names of website visitors, their medical conditions, and their prescriptions.[28]

41. Following the Walgreens incident, Bonobos, a men's clothing retailer, announced that it was eliminating data sharing with a Session Replay Provider after it was discovered that the Session Replay Provider was capturing credit card details, including the cardholder's name and billing address, the card's number, expiration, and security code from the Bonobos' website.[29]

42. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.[30] In announcing this decision, Apple stated: "Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity."[31]

[27] Nitasha Tiku, The Dark Side of 'Replay Sessions' That Record Your Every Move Online, WIRED (Nov. 16, 2017), https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/.
[28] Englehardt, *supra* note 19.
[29] Tiku, *supra* note 27.
[30] Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), https://techcrunch.com/2019/02/07/apple-glassbox-apps/.
[31] *Id.*

D. Noom Secretly Wiretaps its Website Visitors' Electronic Communications.

43. Noom operates the website www.noom.com, as well as all of its subpages. Noom markets itself as a digital health and wellness platform for individuals to lose weight and lead healthier lives.

44. Noom is a subscription-based service, offering a 14-day free trial and various monthly subscription plans.[32] The first step to signing up for Noom's services is taking a 10-minute online quiz where website visitors provide Noom with information about their height, weight, gender, age, why they want to lose weight, how active they are, how often they eat, and whether they are at risk for certain health issues.[33]

45. However, unbeknownst to the millions of individuals perusing Noom's website, Noom intentionally procures and embeds various Session Replay Codes from Session Replay Providers on its website to track and analyze website user interactions with www.noom.com and its subpages.

46. One such Session Replay Provider that Noom procures is FullStory.

47. FullStory is the owner and operator of a Session Replay Code titled FullStory Script, which records all website visitor actions, including information typed by the website users while on the website. Such information can include names, emails, phone numbers, addresses, social security numbers, date of birth, and more; research by the Princeton University Center for Information Technology Policy found that "text typed into forms is collected before the user

[32] Dawnielle Robinson-Walker & Sarah Davis, *Noom Diet Review 2023: Costs, Benefits and Drawbacks*, Forbes (last updated Feb. 22, 2023), https://www.forbes.com/health/body/noom-diet-review/.
[33] *Id.*

submits the form, and precise mouse movements are saved, all without any visual indication to the user."[34]

48. As a user interacts with any website with the embedded FullStory Script, "each click, tap, URL visit, and every other interaction is sent in tiny little packets to that existing session at FullStory servers."[35] This includes button clicks, mouse movements, scrolling, resizing, touches (for mobile browsers), key presses, page navigation, changes to visual elements in the browsers, network requests, and more.[36]

49. As such, the FullStory Script collects highly personal information and substantive communications that can be linked directly to a website user's identity as it monitors, records, and collects a website user's every move. And similar to other Session Replay Codes, the information collected and recorded by the FullStory Script can then be used to play back a user's journey through a website, showing how they interacted with site navigation, calls to action, search features, and other on-page elements. Put differently, the information the FullStory Script captures can be translated into a simulation video of how a user interacts with a website.

50. Finally, the FullStory Script collects website visitors' IP addresses and geolocation data in a visible and searchable format for websites such as Noom. Indeed, the FullStory Script uses IP addresses "to surface geolocation data" and in turn, "[t]his geolocation data allows users

[34] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.
[35] *Id.*
[36] *How does FullStory capture data to recreate my users' experience?*, FullStory, https://help.fullstory.com/hc/en-us/articles/360032975773-How-does-FullStory-capture-data-to-recreate-my-users-experience-, (last visited Mar. 29, 2023) (hereinafter "FullStory Data Capture").

to segment for sessions by country, state, or city."[37] Put differently, by capturing IP address information, the FullStory Script enables websites such as Noom to search recorded website user sessions by specific locations that is "fairly accurate" at the country and state level, and less so at the city level.[38]

51. Importantly, the FullStory Script captures IP addresses by default and the FullStory Script requires websites such as Noom to manually toggle "Discard user IP addresses" to "off" in the FullStory Script's data capture and privacy settings if they do not want the FullStory Script to maintain IP addresses in a readily visible and searchable manner.[39] And even if a website chooses to discard user IP addresses, this does not stop the FullStory Script from using the IP addresses collected during a website session to collect other location data such as country or state.[40] Nor is this feature retroactive. If the FullStory Script has already captured IP addresses, they will remain searchable to clients until the client exceeds their "product analytics retention period and have been deleted."[41]

52. Given the breadth of information the FullStory Script collects, including a website user's IP address and geolocation data, it is inevitable that Noom knows it is capturing, collecting, and recording the Website Communications of Pennsylvania residents. Indeed, once a website installs the FullStory Script, that code acts as a secret wiretap that sends users' Website Communications to FullStory in real time, instantly reporting every keystroke, movement, click, and/or moment of inactivity to the FullStory server.

---

[37] *IP Address & Geolocation*, FullStory, https://help.fullstory.com/hc/en-us/articles/360045926353-IP-Address-Geolocation (last visited Mar. 29, 2023).
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*

53. Noom's procurement and use of FullStory's Session Replay Code, and procurement and use of other Session Replay Codes through various Session Replay Providers, is a wiretap in violation Pennsylvania statutory and common law.

E. Plaintiff's and Class Members' Experience.

54. Plaintiff has visited www.noom.com and certain of its subpages on her computer while in Pennsylvania prior to filing this action.

55. While visiting Noom's website, Plaintiff fell victim to Defendant's unlawful monitoring, recording, and collection of Plaintiff's Website Communications with www.noom.com prior to the filing of this actions.

56. Unknown to Plaintiff, Noom procures and embeds Session Replay Code on its website. In particular, the FullStory Script was operative on Noom's website and subpages during Plaintiff's visits to Noom's website.

57. During a visit by Plaintiff to www.noom.com and its subpages, Plaintiff browsed for different products for sale and signed up for a trial membership. Plaintiff communicated with Noom's website by using her mouse to hover and click on certain services and typing her personal information in text fields.

58. When signing up for her trial membership with Noom, Plaintiff was required to complete a 10-minute quiz where Noom asked questions relating to her weight loss goals, her gender, age, height, weight, lifestyle, marital status, health conditions, her weight loss goals. Plaintiff communicated with Noom by using her mouse to click on certain answers and keyboard to enter her personal information in text fields. At the end of the quiz, Noom asked Plaintiff to enter her email address in order to receive a copy of the results of her quiz.

59. The Session Replay Code instantaneously captured her Website Communications throughout her visit. Indeed, through Noom's procurement of Session Replay Code, Plaintiff's Website Communications were automatically and secretly intercepted while using Noom's website. Further, without her consent, Noom procured Session Replay Providers to obtain certain information about her device, browser, and create a unique ID and profile for her.

60. Further, without her consent, Noom procured Session Replay Providers to obtain certain information about her device and browser, and create a unique ID and profile for her.

61. Thus, when Plaintiff visited Noom's website, the contents of her communications with the website were intercepted by Session Replay Code and simultaneously transmitted to Session Replay Providers.

62. The Session Replay Codes operate in the same manner for all putative Class members.

63. Like Plaintiff, each Class member visited www.noom.com and its subpages with Session Replay Code embedded in it, and those Session Replay Codes intercepted the Class members' Website Communications with www.noom.com by sending hyper-frequent logs of those communications to Session Replay Providers.

64. Even if Noom masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

65. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves

through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

66. The Session Replay Code procured by Noom is an electronic, mechanical, or other analogous device for purposes of WESCA in that the Session Replay Code, monitors, collects, and records the content of electronic computer-to-computer communications between Plaintiff's mobile computer and/or mobile device and the computer servers and hardware utilized by Noom to operate its website.

67. Alternatively, even if the Session Replay Code itself were not a device for purposes of WESCA, the Session Replay Code is software designed to alter the operation of a website visitor's computer or mobile phone by instructing the hardware components of that physical device to run the processes that ultimately intercept the visitor's communications and transmit them to the third-party Session Replay Provider, without the visitor's knowledge.

68. The Session Replay Code procured by Noom is not a website cookie, analytics tool, tag, web beacon, or other similar technology. Instead, the data collected by the Session Replay Code identified specific information inputted and content viewed, and thus revealed personalized and sensitive information about website visitors' Internet activity and habits. As such, by the very nature of its operation, the Session Replay Code is a device used to intercept electronic communications.

69. The Website Communications intentionally monitored, collected, and recorded by Noom was content generated through Plaintiff's and Class Members' use, interaction, and communication with Noom's website relating to the substance and/or meaning of Plaintiff's and Class Members' communications with the website, i.e., mouse clicks and movements, keystrokes, search terms, information inputted by Plaintiff and Class Members, and pages and content clicked

on and viewed by Plaintiff and Class Members. This information is "content" as defined by the Pennsylvania Wiretapping and Electronic Surveillance Control Act and is not merely record information regarding the characteristics of the message that is generated in the course of the communication, nor is it simply information disclosed in the referrer headers. The mere fact that Noom values this content, and monitors, intercepts and records it, confirms these communications are content that convey substance and meaning to Noom, and in turn, any Session Replay Provider that receives the intercepted information.

F. Plaintiff and Class Members Did Not Consent to the Interception of Their Website Communications.

70. Plaintiff and Class Members did not provide prior consent to Noom's interception of their Website Communications, nor could they, as the interception begins *immediately* upon arriving at www.noom.com.

71. As the 2017 study recognized, the extent of data collected by Session Replay Code "far exceeds user expectations [1]; text typed into forms is collected before the user submits the form, and precise mouse movements are saved, all without any visual indication to the user."[42]

72. Noom does not ask website visitors, including Plaintiff and Class Members, for prior consent before wiretapping their Website Communications. Indeed, Plaintiff and Class Members have no idea upon arriving at the Website that Noom is using Session Replay Code to monitor, collect, and record their Website Communications because the Session Replay Code is seamlessly incorporated and embedded into Noom's Website.

73. Further, while Noom purports to maintain a "Privacy Policy," and "Terms of Use" the Privacy Policy and Terms of Use are insufficient for Plaintiff and Class Members to furnish

[42] Englehardt, *supra* note 19.

prior consent. First, at no point prior to the end of the quiz that Noom asks website visitors to take, does Noom ask website visitors to agree to its Privacy Policy or Terms of Use .Because the wiretapping begins the moment a website user visits www.noom.com and Noom does not ask website visitors to agree to the Privacy Policy and Terms of Use until after they have already been wiretapped, Plaintiff and Class Members had no opportunity to review the Privacy Policy before they were wiretapped and therefore cannot provide insufficient and subsequent consent after the wiretapping has already occurred.

74. Further, for those website visitors who do not complete Noom's quiz, a reasonable person would not be on notice of the terms of Noom's Privacy Policy or Terms of Use by way of normal interaction with the Website. Noom's Privacy Policy and Terms of Use are contained on the homepage of www.noom.com, buried at the very bottom of the website in tiny, non-contrasting font that is unobtrusive and easy to overlook. As such a reasonable person could browse Noom's website without ever being on notice of its purported Privacy Policy and Terms of Use.

CLASS ACTION ALLEGATIONS

75. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

> All natural persons in Pennsylvania whose Website Communications were captured in Pennsylvania through the use of Session Replay Code embedded in www.noom.com.

76. Excluded from the Class are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

77. **Numerosity:** The members of the Class are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of Noom or the Session Replay Providers.

78. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: (a) whether Defendant procures Session Replay Providers to intercept Noom's website visitors' Website Communications; (b) whether Noom intentionally discloses the intercepted Website Communications of its website users; (c) whether Defendant acquires the contents of website users' Website Communications without their consent; (d) whether Defendant's conduct violates Pennsylvania Wiretap Act,18 Pa. Cons. Stat. § 5701, *et seq*.; (e) whether Plaintiff and the Class members are entitled to equitable relief; and (f) whether Plaintiff and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

79. **Typicality:** Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each member of the Class had their communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the members of the Class typical of one another.

80. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and her counsel are committed to vigorously

prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members of the Class.

81. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

82. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant intercepted Plaintiff's and Class members' Website Communications, then Plaintiff and each Class member suffered damages by that conduct.

83. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through Noom's books and records or the Session Replay Providers' books and records.

COUNT I
Violation of Pennsylvania Wiretap Act
18 Pa. Cons. Stat. § 5701, et. seq.

84. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

85. Plaintiff brings this claim individually and on behalf of the Class.

86. The Pennsylvania Wiretap Act (the "Act") prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

87. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

88. "Intercept" is defined as any "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. Cons. Stat. § 5702.

89. "Contents" is defined as "used with respect to any wire, electronic or oral communication, is any information concerning the substance, purport, or meaning of that communication." 18 Pa. Cons. Stat. § 5702.

90. "Person" is defined as "any individual, partnership, association, joint stock company, trust or corporation." 18 Pa. Cons. Stat. § 5702.

91. "Electronic Communication" is defined as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." 18 Pa. Cons. Stat. § 5702.

92. Noom is a person for purposes of the Act because it is a corporation.

93. Session Replay Code like that procured by Noom is a "device" used for the "acquisition of the contents of any wire, electronic, or oral communication" within the meaning of the Act. Courts have held that software constitutes a "device" for purposes of applying wiretap statutes. *See, e.g.*, *United States v. Barrington*, 648 F.3d 1178, 1203 (11th Cir. 2011) (accepting that a keylogger software could be considered a device); *Luis v. Zang*, 833 F.3d 619, 630 (6th Cir. 2016) (accepting that a software could be a "device" for the purpose of the Wiretap Act); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1087 (N.D. Cal. 2015) (concluding that a software was an "electronic, mechanical or other device"); *Klumb v. Goan*, 884 F. Supp. 2d 644, 661-62 (E.D. Ten. 2012) (analyzing spyware software as a device under Wiretap Act); *Shefts v. Petrakis*, 2012 WL 4049484, at *8-9 (C.D. Ill. 2012) (analyzing software as a device under the Wiretap Act).

94. Alternatively, even if the Session Replay Code itself were not considered a "device" under the Act, Noom ultimately "uses" the physical computers and mobile phones of Plaintiff and Class members by sending the Session Replay Code to those devices. In turn, the Session Replay Code instructs those devices to run the physical processes necessary to accomplish the interception of Plaintiff's and Class members' communications and transmission of those communications to the third-party Session Replay Providers.

95. Plaintiff's and Class members' intercepted Website Communications constitute the "contents" of electronic communication[s]" within the meaning of the Act.

96. Noom intentionally procures and embeds Session Replay Code on its website to spy on—automatically and secretly—and to intercept its website visitors' electronic interactions communications with Noom in real time.

97. Plaintiff's and Class members' electronic communications are intercepted contemporaneously with their transmission.

98. Plaintiff's interactions with Noom's website and its subpages, including her directional, selection, and clicking actions (using a mouse, arrow keys, or a finger), the display of information coming from Noom and directed to Plaintiff, and Plaintiff's entry of text into search form fields, were all exchanges of electronic communications between Plaintiff and Noom.

99. Plaintiff's and Class members' intercepted Website Communications therefore constitute the "contents" of "electronic communication[s]" within the meaning of WESCA.

100. By operation of the Session Replay Code on Plaintiff's device, these forms of communications were captured continuously, within milliseconds, and immediately transmitted to and acquired by third-party Session Replay Providers.

101. Plaintiff and Class members did not consent to having their Website Communications wiretapped.

102. Pursuant to 18 Pa. Cons. Stat. 5725(a), Plaintiff and the Class members seek (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

103. Noom's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II
Invasion of Privacy – Intrusion Upon Seclusion

104. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

105. Pennsylvania common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in multiple sections of the Pennsylvania constitution.

106. Plaintiff brings this claim individually and on behalf of the Class.

107. Plaintiff and Class members have an objective, reasonable expectation of privacy in their Website Communications.

108. Plaintiff and Class members did not consent to, authorize, or know about Noom's intrusion at the time it occurred. Plaintiff and Class members never agreed that Noom could collect or disclose their Website Communications.

109. Plaintiff and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

110. Noom intentionally intrudes on Plaintiff's and Class members' private life, seclusion, or solitude, without consent.

111. Noom's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

112. Plaintiff and Class members were harmed by Noom's wrongful conduct as Noom's conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

113. Noom's conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

114. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff's and Class members' property.

115. Further, Noom has improperly profited from its invasion of Plaintiff and Class members' privacy in its use of their data for its economic value.

116. As a direct and proximate result of Noom's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

117. Noom's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Class, respectfully request that the Court enter judgment in Plaintiff's and the Class's favor and against Defendant as follows:

A. Certifying the Class and appointing Plaintiff as the Class representative;

B. Appointing Plaintiff's counsel as class counsel;

C. Declaring that Defendant's past conduct was unlawful, as alleged herein;

D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;

E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

Dated: March 29, 2023

Respectfully submitted,

/s/ Gary F. Lynch

Gary F. Lynch
Kelly K. Iverson
Jamisen A. Etzel
Elizabeth Pollock-Avery
Nicholas A. Colella
Patrick D. Donathen
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Telephone: 412-322-9243
Facsimile: 412-231-0246
gary@lcllp.com
kelly@lcllp.com
jamisen@lcllp.com
elizabeth@lcllp.com
nickc@lcllp.com
patrick@lcllp.com